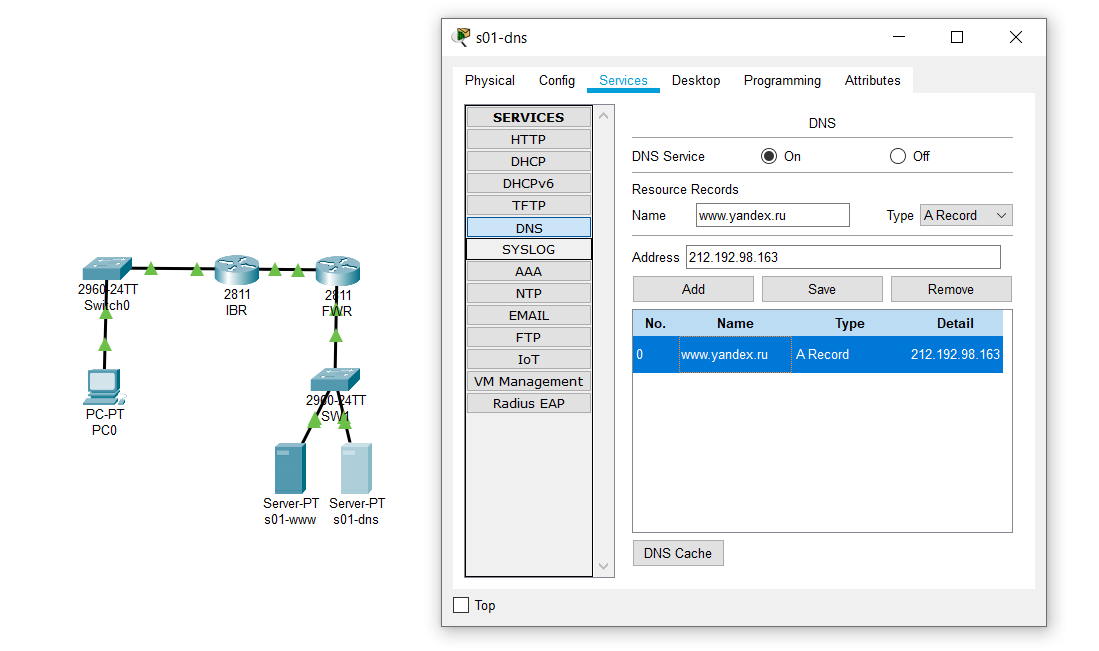
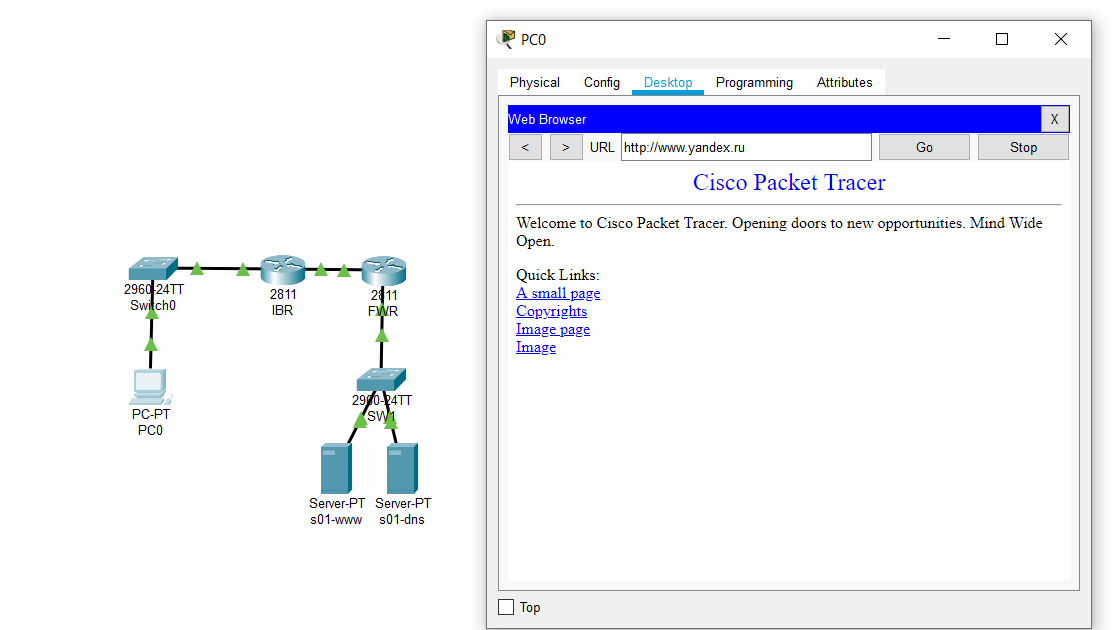
Дровосеков Д.А. КМБ-16

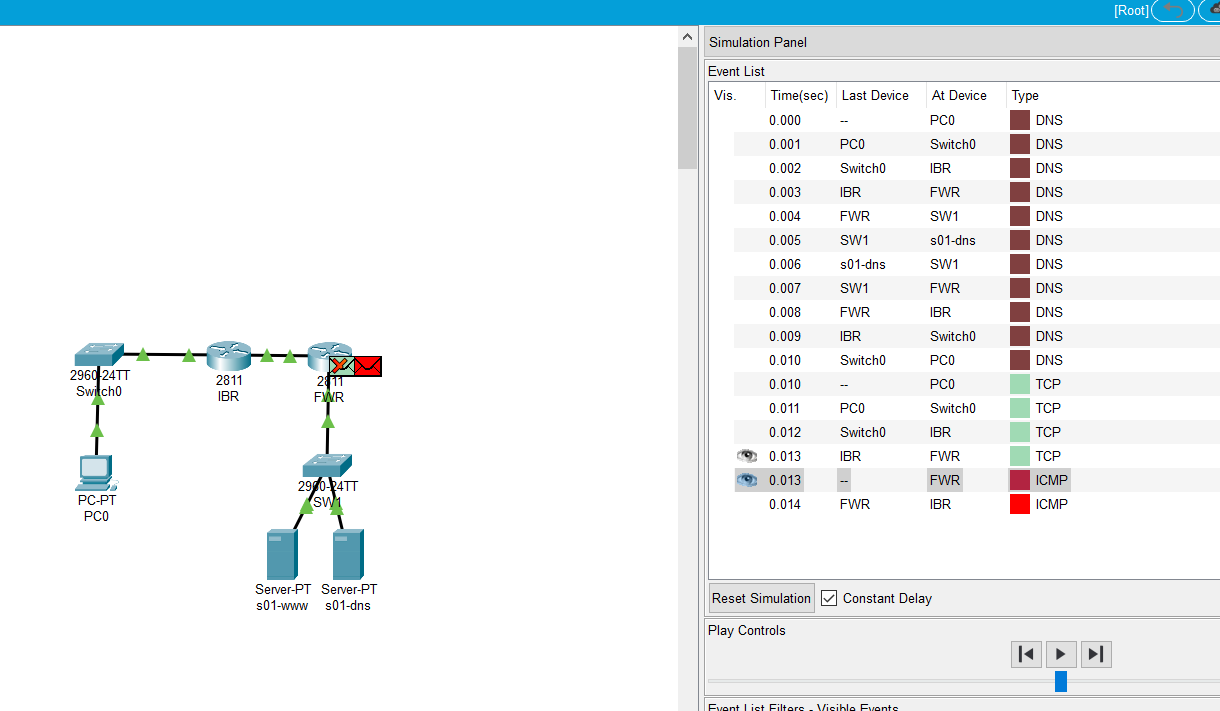
Включим на DNS-сервере DNS, обратимся к ресурсу.



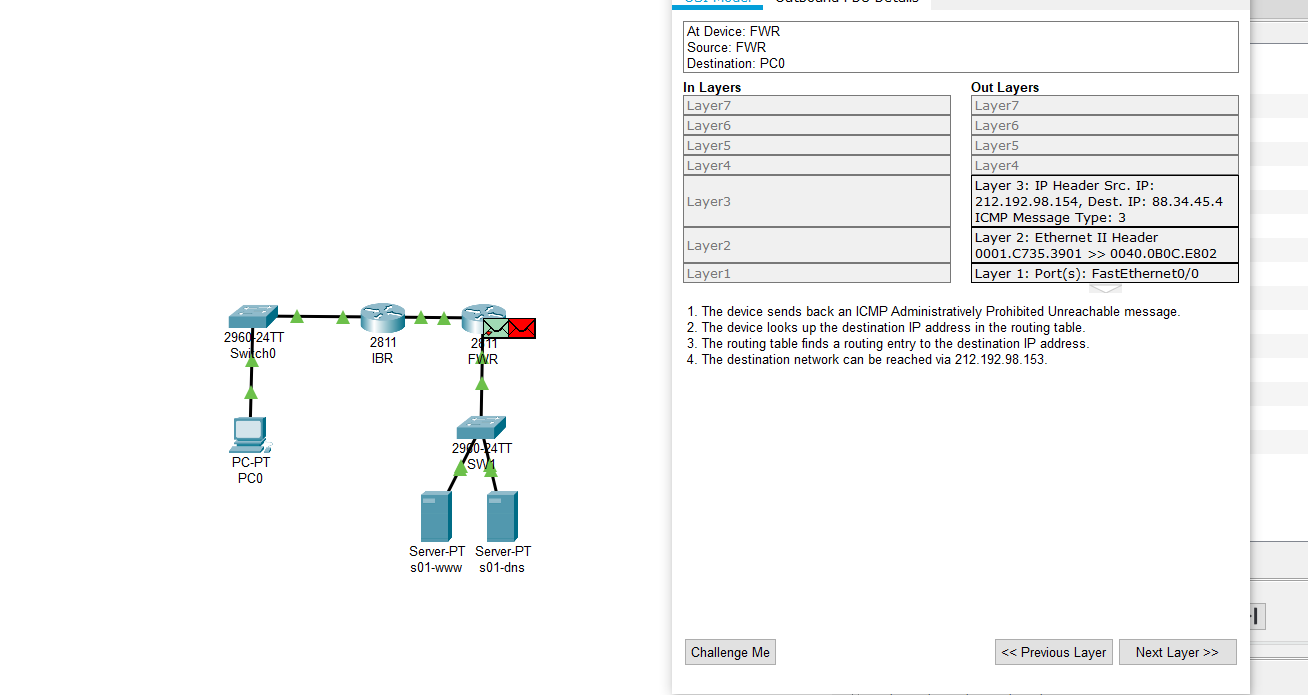
Ответ доходит до клиента.



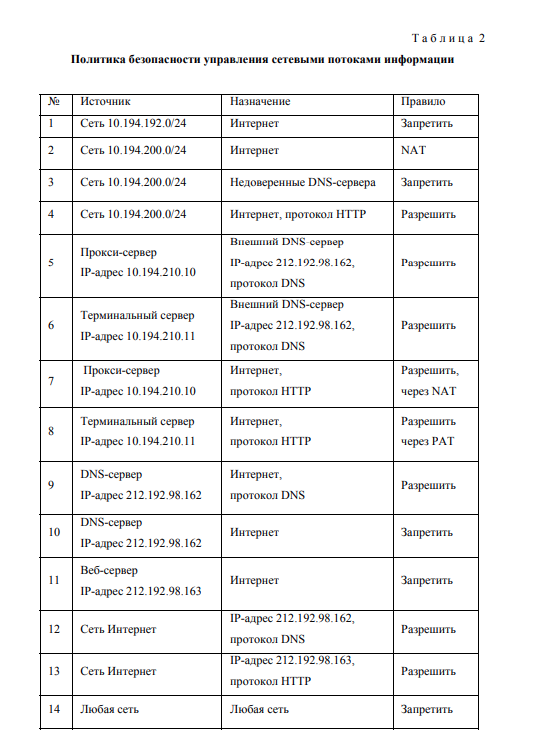
Пакет с HTTP запросом блокируется на роутере.



Содержание пакета



1. Проанализировать политику безопасности управления информационными потоками, представленную в табл. 2.



10.194.200.0/24 доступ в Интернет по технологии NAT

10.194.192.0/24 доступ в Интернет запрещен, осуществляется через 10.194.210.11

10.194.210.10 прокси-сервер

выделяются IP-сети 212.192.98.168/29 и 212.192.98.154/32 для реализации NAT

212.192.98.162 DNS-сервер в сегменте ДМЗ

212.192.98.163 WWW-сервер в сегменте ДМЗ

2. Дополнить политику безопасности управления информационными потоками правилами для проектируемой вами электронной почтовой системы.

Для передачи электронных писем применяются протоколы SMTP и POP3, которые используют протокол TCP на портах 25 и 110

ip access-list extended acl-LAN

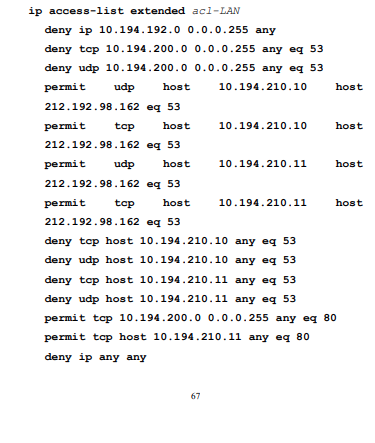
permit tcp host (ip-client) host (ip-server) eq 25

ip access-list extended acl-DMZ

permit tcp host (ip-server) host (ip-client) eq 110

3. Обеспечить доступ к сети Интернет из сетей филиалов через ГВС. При необходимости внести изменения в политику безопасности управления информационными потоками.

Для обеспечения доступа из сети 10.194.192.0/24 в Интернет необходимо заменить



На

permit tcp 10.194.192.0 0.0.0.255 host 212.192.98.162 eq 53

permit udp 10.194.192.0 0.0.0.255 host 212.192.98.162 eq 53

deny tcp 10.194.192.0 0.0.0.255 any eq 53

deny udp 10.194.192.0 0.0.0.255 any eq 53

permit tcp 10.194.192.0 0.0.0.255 any eq 80